

FortiHypervisor Administration Guide

VERSION 1.0

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

CLI REFERENCE

<http://cli.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



February 10, 2017

FortiHypervisor Administration Guide

Version 1.0

Table of Contents

CHANGE LOG	4
INTRODUCTION	5
FORM-FACTORS	5
SPU SUPPORT	6
INSTALLING THE ISO VERSION.....	7
CREATING USB BOOT MEDIA.....	7
INSTALLING FORTIHYPERVISOR.....	8
INSTALLING FORTIHYPERVISOR IN VMWARE ESXI.....	8
GETTING STARTED	13
BASIC CONFIGURATION	13
ADVANCED CONFIGURATION	16
VIRTUAL NETWORKING.....	18
EXTERNAL INTERFACES.....	18
VIRTUAL SWITCH.....	19
PROVISIONING VMS.....	21
INSTALLING FORTINET VMS	21
INSTALLING THIRD PARTY VMS	24
APPENDIX A.....	27
TESTED FORTINET VM CONFIGURATIONS.....	27
TESTED THIRD PARTY VM CONFIGURATIONS.....	27

Change Log

Date	Change Description
2017-02-10	Initial revision
2017-03-01	Minor corrections and addition of additional CLI examples

Introduction

The FortiHypervisor Hybrid Virtual Appliance enables rapid service delivery for enterprise and MSPs through the use of virtualization technology. Built to deliver multiple virtualized network functions (VNFs), FortiHypervisor consolidates advanced networking and security services, eliminating the need for multiple CPE while enabling on-demand service delivery.

FortiHypervisor is available as Fortinet SPU accelerated hybrid appliances and also in software format for install on generic x86 platforms. In appliance format, a powerful Intel processor combined with SPU hardware acceleration delivers the high security performance that customers have come to expect from Fortinet. Ample storage and memory produce excellent compute, network and security performance for the most intensive tasks.

FortiHypervisor supports an industry leading range of virtual network functions with native Fortinet VNFs and support for standards based third party VMs.

Form-factors

FortiHypervisor is available in two form-factors to allowing customers to select the most appropriate solution for their requirements.

Appliance

FortiHypervisor comes in a range of physical appliances suitable for small office / retail deployments (vCPE) all the way up to the datacenter and MSP network core. The models come with different performance ratings, amounts of Hard Drive space, RAM and network access ports.

Software

FortiHypervisor is available as a bare metal hypervisor ISO image which can be installed on selected whitebox hardware.



Any selected hardware should be validated against the supported hardware list and should meet the minimum hardware specification lists below.

Whilst a minimum specification is provided, consideration should be made towards the VMs which will be installed as these may have additional performance and resource requirements.

If unsure, please validate your hardware selection with Fortinet Support before proceeding.

Supported Hardware

The following hardware components are supported by FortiHypervisor Software:

CPU

Intel
AMD

Network

E1000/E1000e
EGB
IXGBE
TG3
BNX2
RTL8169

SCSI

MEGARAID_SAS
MPT2SAS
FUSION_SAS
HPSA



Any hardware not listed as supported should be submitted to Fortinet as an NFR for consideration for inclusion.

SPU support

The following requirements must be met in order for traffic to be accelerated on the FortiHypervisor appliance:

- Appliance must contain an NP6 SPU (e.g. FHV-500D or FHV-2500E models)
- VM vNIC model must be set to the VirtIO hardware type
- VM interface must be set to a passthrough virtual switch

You can verify if traffic is being offloaded by running `diag sys session list` in the guest FortiOS VM.

Offloaded output will look like this:

```
serial=00000026 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=130/131, ipid=131/130,
vlan=0x0000/0x0000
vlifid=131/130, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
total session 1
```

NP6 SPU limitations

Whilst the majority of NP6 functions have been exposed for use by the guest FortiOS, some functions are not yet implemented. Currently all features of the NP6 are supported by FortiOS KVM with the exception of:

- CAPWAP offloading
- NTurbo offloading
- IP Tunnel offloading

Installing the ISO version

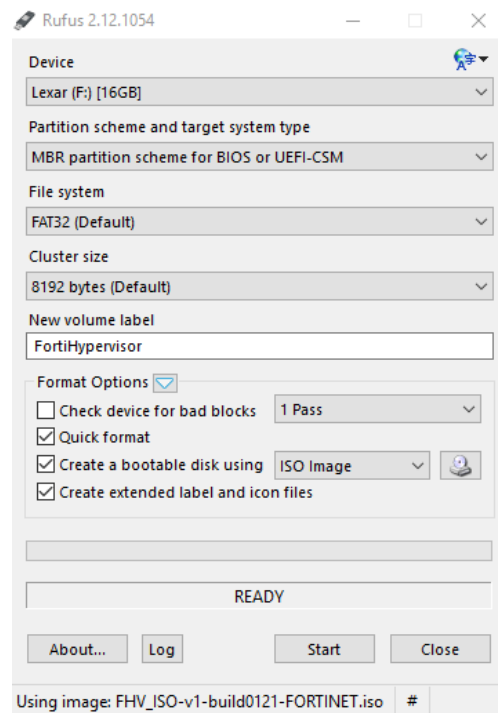
FortiHypervisor is available in ISO format for installation on generic “whitebox” hardware. Download this for the Fortinet support site and burn to a CDROM/DVD for installation. If a CDROM is not available to perform the installation, follow the information in the section

Creating USB boot media

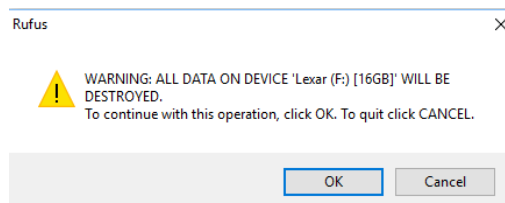
It is possible to write FortiHypervisor to a USB device for installation purposes. To achieve this, download a copy of the USB creation utility Rufus <https://rufus.akeo.ie/>.

Select the USB device to install the ISO Bootable Disk to.

Select “*Create a bootable disk using ISO image*” and click the CD icon to select the source as the downloaded FortiHypervisor ISO image.



Select start and validate the settings before clicking OK to continue with the install of FortiHypervisor to the USB media.



Once complete, this USB device can be used to install FortiHypervisor.

Installing FortiHypervisor

Boot your device with either the CDROM (ISO) or USB installation media. Note that you may need to consult your hardware manufacturer's guide to change the default boot order.

Once booted, assuming the network and disks have been correctly identified, the following prompt will be displayed.

```
FortiHypervisor Installer

Checking disk sda major 8 minor 0 ...

Network Interfaces:
ID      Name      Driver
1       eth0      e1000

Hard Disks:
ID      Name      Size
1       sda       21GB

Please select disk to install.
Press [Enter] to refresh disk list.
ID: _
```

Select the correct disk on which to install FortiHypervisor

```
Installing to disk [sda] will erase all data on it,
Do you want to continue? (y/n)_
```

Accept the prompt to continue (assuming this is the correct disk and you are happy to lose any data currently stored).

```
Installing to disk [sda] will erase all data on it,
Do you want to continue? (y/n)y
Installing OS...
Partitioning disk...
```

The disk partition process will begin. After several minutes, the installation process should complete.

```
Partitioning disk...
Copying files...
100%
Syncing disk...
Installing bootloader...

Press Enter to restart system.
_
```

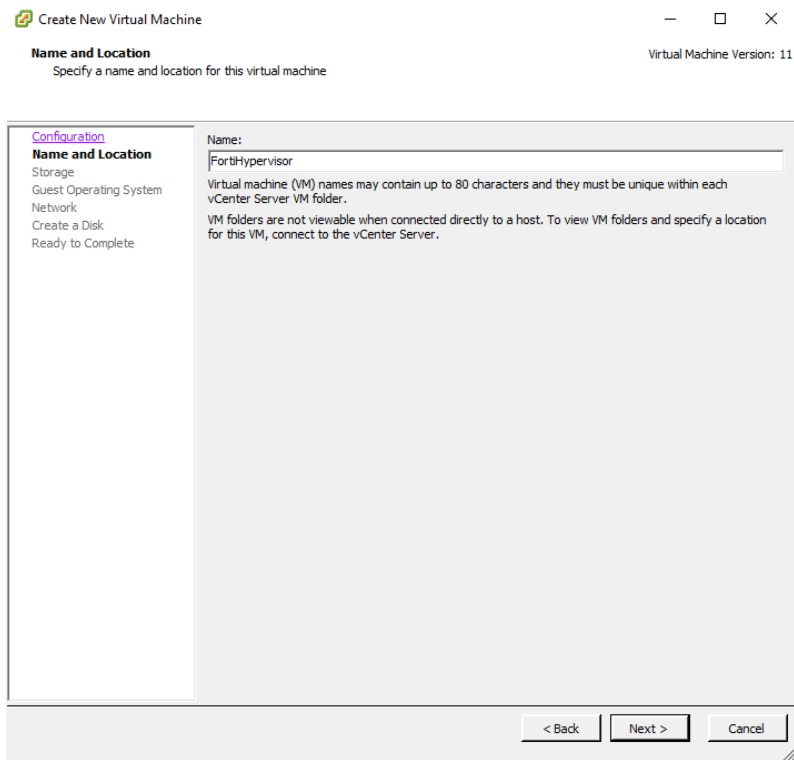
Follow the instructions on screen to complete the install process and reboot.

Continue the configuration process as per hardware appliances.

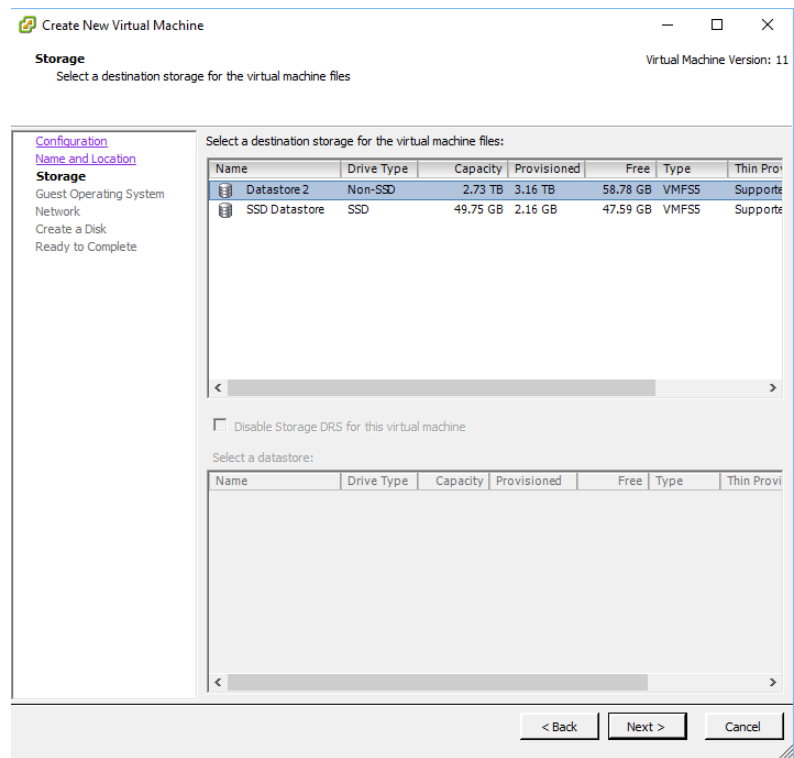
Installing FortiHypervisor in VMWare ESXi

Whilst not recommended for general use, it is possible to install FortiHypervisor into an existing hypervisor such as VMWare ESXi. This is useful for demo purposes and testing.

To install FortiHypervisor in VMWare ESXi, create a new VM



Select the storage destination.



Set the Guest Operating System to Other Linux (64 bit)

The screenshot shows the 'Create New Virtual Machine' wizard at the 'Guest Operating System' step. The left sidebar contains links for 'Configuration', 'Name and Location', 'Storage', 'Guest Operating System' (which is highlighted), 'Network', 'Create a Disk', and 'Ready to Complete'. The main area is titled 'Guest Operating System' with the subtitle 'Specify the guest operating system to use with this virtual machine'. It shows three radio buttons: 'Windows', 'Linux' (which is selected), and 'Other'. Below these is a 'Version:' dropdown menu set to 'Other Linux (64-bit)'. A note states: 'Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.' At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Assign network resources to the VM instance.

The screenshot shows the 'Create New Virtual Machine' wizard at the 'Network' step. The left sidebar is the same as the previous step, with 'Network' highlighted. The main area is titled 'Network' with the subtitle 'Which network connections will be used by the virtual machine?'. It features a 'Create Network Connections' section with a dropdown for 'How many NICs do you want to connect?' set to '1'. Below is a table with columns 'Network', 'Adapter', and 'Connect at Power On'. The first row shows 'NIC 1' connected to 'Public Network' using an 'E1000' adapter, with the 'Connect at Power On' checkbox checked. A note mentions that more than 4 NICs can be added after creation. Another note states that adapter choice affects performance and migration compatibility, advising to consult the VMware KnowledgeBase. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Assign disk resource to the VM instance

The screenshot shows the 'Create New Virtual Machine' wizard at the 'Create a Disk' step. The left sidebar contains links for Configuration, Name and Location, Storage, Guest Operating System, Network, Create a Disk (highlighted), and Ready to Complete. The main area is titled 'Specify the virtual disk size and provisioning policy'. It includes fields for Datastore (Datastore 2), Available space (58.8 GB), and Virtual disk size (20 GB). Three radio buttons are present: Thick Provision Lazy Zeroed (selected), Thick Provision Eager Zeroed, and Thin Provision. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

Create New Virtual Machine

Virtual Machine Version: 11

Create a Disk
Specify the virtual disk size and provisioning policy

Configuration
Name and Location
Storage
Guest Operating System
Network
Create a Disk
Ready to Complete

Datastore: Datastore 2

Available space (GB): 58.8

Virtual disk size: 20 GB

☒ Thick Provision Lazy Zeroed
☐ Thick Provision Eager Zeroed
☐ Thin Provision

< Back Next > Cancel

Review the configuration, “*edit the virtual machine settings before completion*” and click *continue*.

The screenshot shows the 'Create New Virtual Machine' wizard at the 'Ready to Complete' step. The left sidebar contains links for Configuration, Name and Location, Storage, Guest Operating System, Network, Create a Disk, and Ready to Complete (highlighted). The main area is titled 'Click Finish to start a task that will create the new virtual machine'. It includes a table of 'Settings for the new virtual machine:' with fields for Name, Host/Cluster, Datastore, Guest OS, NICs, NIC 1 Network, Disk provisioning, and Virtual Disk Size. At the bottom, there is a checkbox 'Edit the virtual machine settings before completion' (checked) and a warning icon with text: 'Creation of the virtual machine (VM) does not include automatic installation of the guest operating system. Install a guest OS on the VM after creating the VM.' At the bottom are buttons for '< Back', 'Continue', and 'Cancel'.

Create New Virtual Machine

Virtual Machine Version: 11

Ready to Complete
Click Finish to start a task that will create the new virtual machine

Configuration
Name and Location
Storage
Guest Operating System
Network
Create a Disk
Ready to Complete

Settings for the new virtual machine:

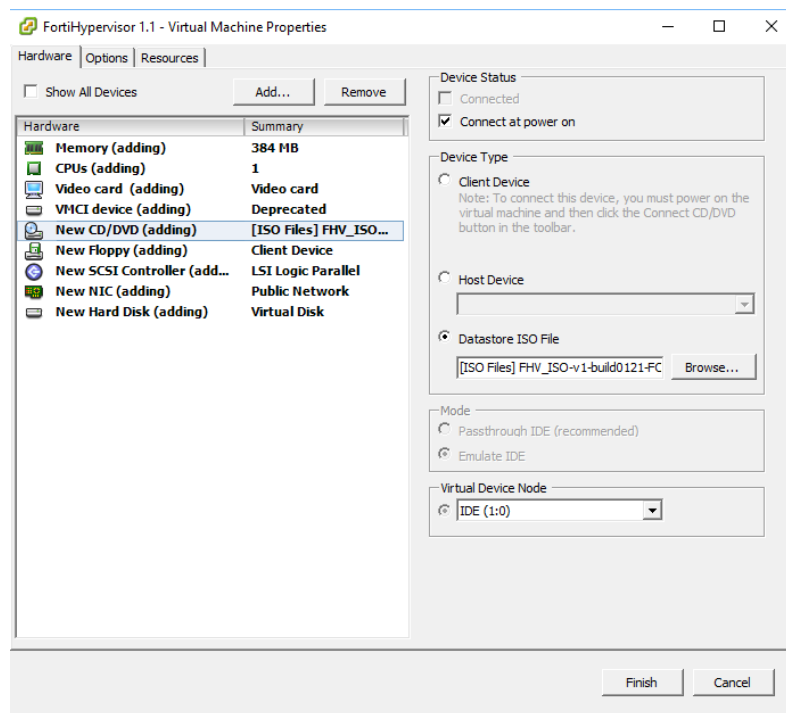
Name:	FortiHypervisor 1.1
Host/Cluster:	localhost
Datastore:	Datastore 2
Guest OS:	Other Linux (64-bit)
NICs:	1
NIC 1 Network:	Public Network
Disk provisioning:	Thick Provision Lazy Zeroed
Virtual Disk Size:	20 GB

☒ Edit the virtual machine settings before completion

⚠ Creation of the virtual machine (VM) does not include automatic installation of the guest operating system. Install a guest OS on the VM after creating the VM.

< Back Continue Cancel

Configure the *Datastore ISO* file to point to the FortiHypervisor install ISO and select *Connect at power on*.



Follow the install process detailed in the section “Installing FortiHypervisor”.

Getting Started

Basic Configuration

This section discusses the installation and use of FortiHypervisor in your network, after completion of the initial setup outlined in the FortiHypervisor model's Quick Start Guide. The section also provides troubleshooting tips and links to other resources..



The following example content is based on the FortiHypervisor 500D. The process is similar for other FortiHypervisor appliances, however variations in model specification may alter which interface settings are available.

The default IP address of the FortiHypervisor *mgmt1* interface is set to 192.168.1.99/24. To perform the initial configuration, connect a device to mgmt1. Configure the device with an IP address to 192.168.1.1/24. The FortiHypervisor should be accessible via SSH or the Web GUI.

The default username is `admin` and password `<blank>`.

Use the GUI or CLI to set the permanent IP address configuration.



The initial configuration may be performed on the serial console. Please see the quick start guide for details.

<http://docs.fortinet.com/fortihypervisor/hardware/>

Configuring the Management IP

Once you have successfully accessed the Web GUI and logged in, the management interface may be set by clicking *System > External Interface* and adjust the IP address settings as required.

The screenshot shows the FortiHypervisor 500D Web GUI. The top bar is green with the device name 'FortiHypervisor 500D' and ID 'FHV5HD3916800061'. The left sidebar has a menu with 'System' selected, and 'External Interface' highlighted. The main area is titled 'Edit Interface' and shows configuration for the 'mgmt1 (90:6C:AC:C4:7A:82)' interface. The 'Addressing mode' is set to 'Manual' (highlighted in green) with 'DHCP' as an option. The 'IP/Network Mask' is '192.168.0.198/255.255.255.0'. Under 'Administrative Access', 'HTTPS', 'PING', 'HTTP', and 'SSH' are checked, while 'SNMP' and 'TELNET' are unchecked. 'Link Status' is 'Up' with a green arrow icon. The 'Type' is 'Physical Interface'. The 'Status' section has a 'Comments' field and 'Interface State' set to 'Enabled' (green arrow icon) with 'Disabled' (red arrow icon) as an option. At the bottom right are 'OK' and 'Cancel' buttons.

To configure via the CLI:

```

config system interface
    edit "mgmt1"
        set type physical
        set ip 192.168.0.198 255.255.255.0
        set allowaccess ping https ssh snmp http
    next
end

```



In 1.0 GA, the configuration of the management interface was achieved via the network settings wizard on the Dashboard.

Reconnect the FortiHypervisor device to the network which has just been configured and reconnect to the new GUI IP address.

Configuring DNS

Once complete, configure DNS for the correct settings for your network (not required if DHCP configuration is set)

FortiHypervisor 500D FHV5HD3916800061

Dashboard | Network Settings

System (selected) | DNS Settings

External Interface | Use FortiGuard Servers Specify

DNS (selected) | Primary DNS Server 8.8.8.8

Static Route | Secondary DNS Server 8.8.4.4

Virtual Switch | Local Domain Name

Storage | Apply

Settings

Admin | Image | Virtual Machine

To configure via the CLI:

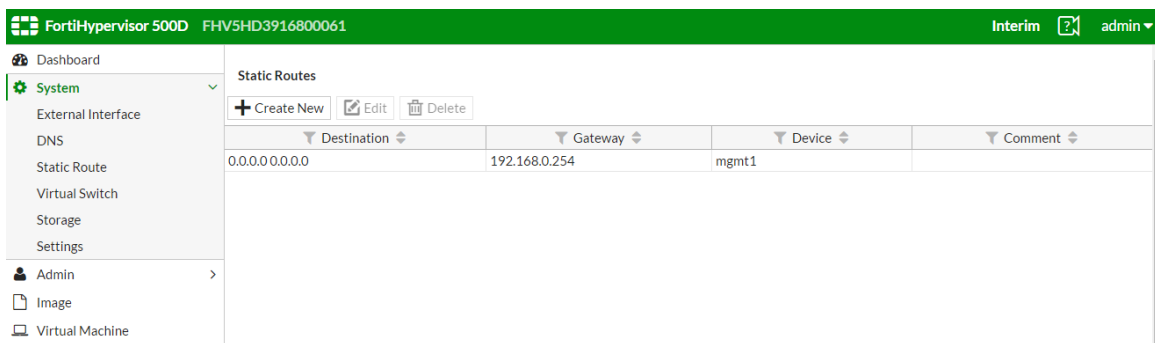
```

config system dns
    set primary 8.8.8.8
    set secondary 8.8.4.4
end

```

Configuring the Default Route

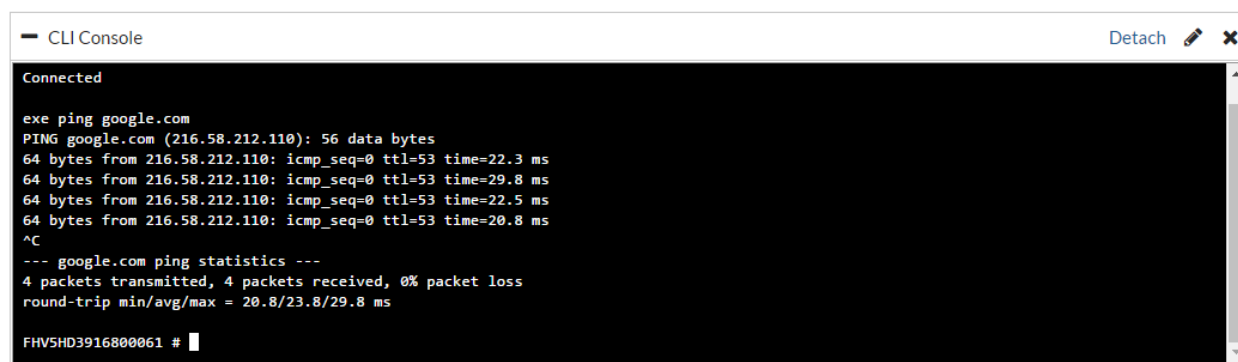
Complete the basic network configuration by setting the correct default route for your network.



To configure via the CLI:

```
config router static
  edit 1
    set gateway 192.168.0.254
    set device "mgmt1"
  next
end
```

Once complete, verify external connectivity, ping an external IP from the Dashboard console



Admin timeout

FortiHypervisor is an appliance designed to host virtual network functions securely. As a result, in line with other Fortinet products and general best practice the default administration timeout is set to 5 minutes. When commissioning FortiHypervisor appliances, it may be necessary to increase the GUI login idle timeout. This is often necessary as the admin session can timeout when uploading large VM images or ISO files. This will cause the upload to fail.

For version 1.0, this is achieved on the CLI.

```
config system global
  set admintimeout 100
end
```

License Information

To automatically provision registered licenses into Fortinet VMs from the FortiHypervisor GUI, it is necessary to register the FortiHypervisor in your FortiCare Support account.

On the Dashboard, select *[Update]* in the License Information widget.

License Information

Account:

VM License:

[Update]

In the Update License Information dialogue, enter your FortiCare Support Account details.

Update License Information

Name:

Password:

OK Cancel

Once registered, your VM licenses will be displayed in the Dashboard and will be able to be provisioned into Fortinet VMs.

License Information

Account: cwindor@fortinet.com

VM License: FAZ-VM0000059960, FCHV020000059964, FCHV020000059965, FCHV020000060108, FEVM010000061259, FEVM010000061260, FEVM020000059950, FEVM020000059959, FEVM020000060092, FEVM020000060093, FGVM010000081785, FMG-VM0A16000931, FO-SVM0000006325

[Update]

Advanced Configuration

REST API

One of the key advantages of the FortiHypervisor platform is its ability to scale vertically and horizontally. Horizontal scaling can be achieved programmatically by deploying many FortiHypervisor instances and associated virtual network functions in parallel. FortiHypervisor exposes programmatic feature configuration via a RESTful Web API. The following RESTful APIs are supported by FortiHypervisor:

- **CMDB API**
 - Retrieve object meta data (default, schema)
 - Retrieve object/table (with filter, format, start, count, other flags)
 - Create object
 - Modify object
 - Delete object
 - Clone object
 - Move object
- **Monitor API**
 - Retrieve/Reset endpoint stats (with filter, start, count)
 - Perform endpoint operations
 - Upload/Download files
 - Restore/Backup config

- Upgrade/Downgrade firmware
- Restart/Shutdown FHV
- Create/Modify/Delete VMs
- Start/Restart/Shutdown/PowerOff VMs

Detailed documentation of the FortiHypervisor REST API is available via the [Fortinet Developer Network](#).

Virtual Networking

External Interfaces

External interfaces refer to the NICs directly attached to the FortiHypervisor platform. External interfaces allow the FortiHypervisor host and associated virtual network functions and VMs to communicate with the outside world, via a connection to an upstream network.

All physical interfaces on FortiHypervisor can be viewed and configured under *System > External Interfaces*.

Status	Name	Members	IP/Netmask	Type	Access	Ref.
+	mgmt1		192.168.0.198 255.255.255.0	Physical	PING HTTPS SSH HTTP	2
+	mgmt2		192.168.2.99 255.255.255.0	Physical	PING HTTPS SSH HTTP	0
+	port1			Physical		1
+	port2		0.0.0.0 0.0.0.0	Physical		0
+	port3		0.0.0.0 0.0.0.0	Physical		0
+	port4		0.0.0.0 0.0.0.0	Physical		0
+	port5		0.0.0.0 0.0.0.0	Physical		0
+	port6		0.0.0.0 0.0.0.0	Physical		0
+	port7		0.0.0.0 0.0.0.0	Physical		0
+	port8		0.0.0.0 0.0.0.0	Physical		0
+	port9		0.0.0.0 0.0.0.0	Physical		0
+	port10		0.0.0.0 0.0.0.0	Physical		0
+	port11		0.0.0.0 0.0.0.0	Physical		0
+	port12		0.0.0.0 0.0.0.0	Physical		0
+	port13		0.0.0.0 0.0.0.0	Physical		0
+	port14		0.0.0.0 0.0.0.0	Physical		0
+	port15		0.0.0.0 0.0.0.0	Physical		0
+	port16		0.0.0.0 0.0.0.0	Physical		0

Creating new interfaces

It is possible to create new interface types for which can be connected to guest VMs:

802.3ad Interfaces

IEEE 802.3ad link aggregation enables ethernet interfaces to be grouped at the physical layer to form a single link layer interface, also known as a link aggregation group (LAG) or bundle. This interface uses Link Aggregation Control Protocol (LACP) to aggregate the interface and control the load distribution or packets across the interface group. Up to 10 interfaces can be configured in LAG.

Packets are load distributed by using a hashing algorithm based on the source/destination IP and ports of the packet.

An 802.3ad interface group provides both resilience and scaling of internet throughput.

Redundant interfaces

The redundant interface configuration allows multiple interfaces to be grouped together in a similar way to 802.3ad, however they are not all active. Redundant interfaces operate in an Active-Passive configuration only, failing over when the active link fails.

A redundant interface group provides resilience only.

Virtual Switch

There are two modes that a switch interface can operate in the FortiHypervisor.

Bridge

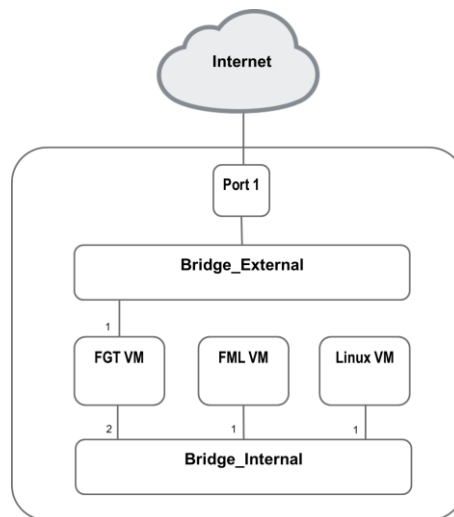
The most common configuration mode is to associate an interface as part of a bridge where all interfaces configured in that bridge are part of a shared Layer2 broadcast domain.

External Interfaces (Physical, VLAN, 802.3ad and Redundant) can all be part of a bridge virtual switch. A virtual machine interface can be connected to a bridge with or without an External Interface

In the following example, the FortiGate VM Port1 interface is connected to the Virtual Switch “Bridge_External” which is also connected to the External Interface Port 1 which is a physical interface connected to the internet.

There is a second Virtual Switch “Bridge_Internal” which is only used to internally connect VM interfaces.

For the FortiMail and Linux VM to communicate with the Internet, the FortiGate would need to be configured to route and allow this traffic.

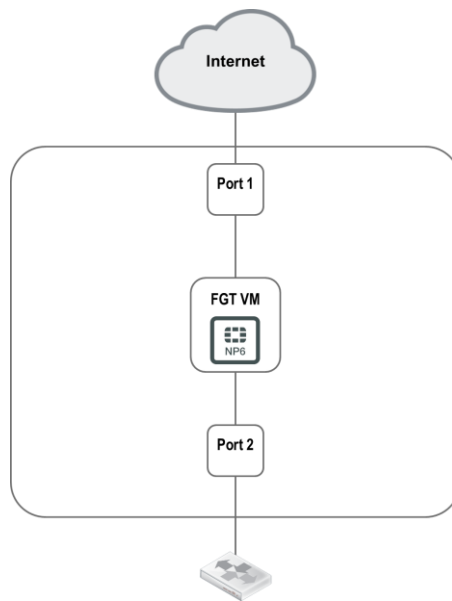


The configuration described would appear as shown below in the FortiHypervisor GUI. Note that only Bridge_External has an External Interface connected as Bridge_Internal is purely a virtual switch used to interconnect the VMs.

FortiHypervisor 500D FHV5HD3916800061			
Dashboard	+ Create New Edit Delete		
System			
External Interface	Name	External Interface	Virtual Machine Interface
DNS	Bridge_External	port1	FortiOS_5.6_Beta2_Boot.port1
Static Route	Bridge_Internal		FortiOS_5.6_Beta2_Boot.port2, FortiMail.port1, CentOS7.port1
Virtual Switch			

Passthrough

Passthrough mode directly connects a VM interface to an External Interface without the need for an intermediary Virtual Switch. Passthrough mode is a pre-requisite for FortiOS to offload network performance to the NP6 SPU.



Provisioning VMs

This section will detail the methods for installing FortiGate/FortiOS and other Fortinet VNFs and thirty party VMs into FortiHypervisor.

There are 2 areas in which VMs are configured in FortiHypervisor.

Image

The Image menu, is where Fortinet and third party VM disks are uploaded [Upload] and empty disks created [Create New]. This is also where ISO files can be uploaded for use in installing an OS into a virtual machine.

VM disks should be uploaded in uncompressed KVM QCOW2 format and CD/DVDs in ISO9660 format.

Virtual Machines

The Virtual Machines menu is where VM are configured. A VM configuration includes definition of the number of CPUs and RAM provisioned, disks to be used, any CDROMs mounted and which network interfaces configured.

For systems with an active FortiCare support account attached, It is possible to provision a new Fortinet VM directly from FortiGuard using the Virtual Machines menu, bypassing the need to manually upload the disk images.



Note that when provisioning CPU resource, it is possible to overcommit resource i.e. so more CPUs are specified that are physically available. Please be aware of the consequence of such configuration. Memory cannot be overcommitted at this time and is limited to being configured to 100% of the available resource minus 2GB which is reserved for system use.

Installing Fortinet VMs

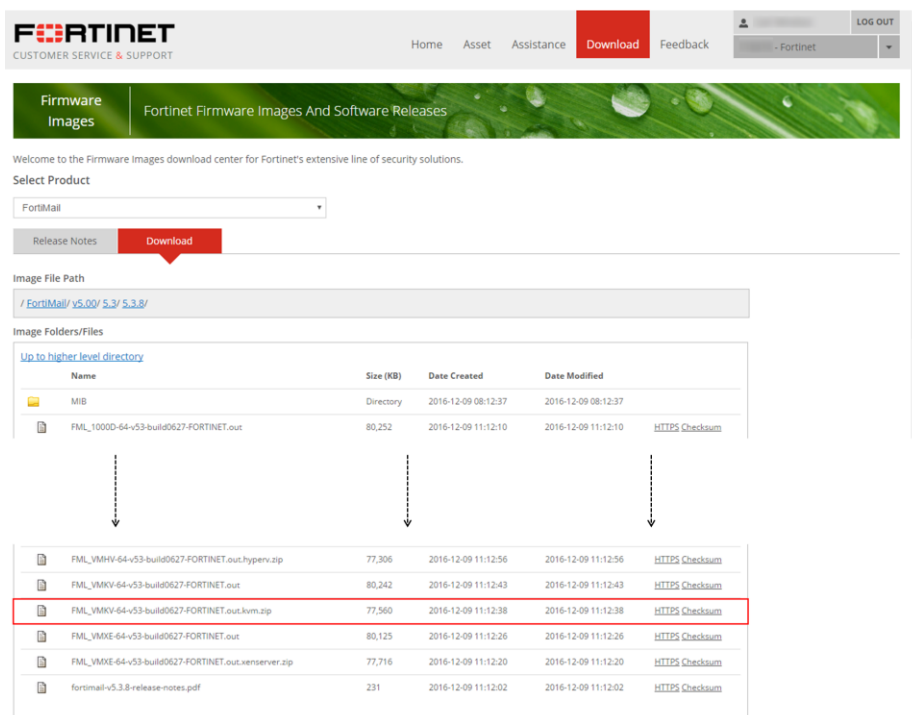
Automatic Import

Automatic import will be provided at in a future release via the Virtual Machine > Import button.

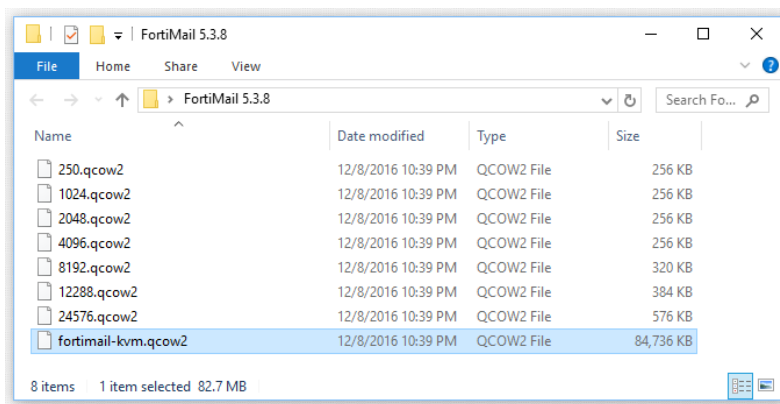
Manual Upload

If a Fortinet VM is not available via the automatic import method shown above, it is possible to manually import the Fortinet VM.

Locate and download the KVM version of the required VM from the *Download > Firmware Images* section of the [Fortinet Support](#) site e.g. for FortiMail 5.3.8:



Once downloaded, extract the zip file to a folder on your management computer.



VMs such as FortiOS, FortiManager and FortiCache only have a single boot disk and data disks need to be created manually to the required size. Some VMs such as FortiMail have pre-defined disk templates of varying sizes which can optionally be used to provision the data disks for a VM install.

fortimail-kvm.qcow2 FortiMail boot disk
250 - 24576.qcow2 FortiMail data disk template in sizes from 250GB to 24TB

Upload the boot disk to the FortiHypervisor by selecting Image > [Upload].

Repeat the process for the data disk using one of the provided templates as shown:

Alternatively, manually create a disk with whatever disk size is required by selecting *Image* > *[Create New]*.

Once the disks have been configured, proceed to the *Virtual Machine* > *[Create New]* to provision the VM.

- CPU:** Select the number of CPUs to suit your environment and VM license
- Memory:** Select the amount of memory to suit your environment and VM license
- Boot Order** Select the boot order of Hard-Disk or CDROM. In the Fortinet VM case this is always Hard-Disk.
- License:** If the FortiHypervisor is correctly associated with a FortiCare account, any supported VM licenses should appear here. These licenses can be selected and automatically configured into the VM using cloud-init for supported Fortinet VMs.
- AutoStart:** Start the VM once configuration has been completed?
- Disk:** Select Create New and bind the previously uploaded Boot disk and data disk(s) (VM dependent)
- Select the disk type according to the VM being configured.
 - For Fortinet VMs this is normally virtio however see Appendix X for exceptions.
- Interface:** Select Create New and bind the appropriate Virtual Switch interfaces to the VM

- Select the interface type according to the VM being configured.
- For Fortinet VMs this is normally virtio-net however, refer to Appendix X for exceptions.

FortiHypervisor 500D FHV5HD3916800061

Dashboard
System
Admin
Image
Virtual Machine

New

Name: FortiMail
CPUs: 2
Memory(MB): 2048
Boot Order: Hard-disk
License: FEVM010000061260

☒ Auto Start

Disk

+ Create New Edit Delete

Name	File	Type	Interface
disk1	/HDD1/FortiMail_Boot	disk	virtio
disk2	/HDD1/FortiMail_Data	disk	virtio

Interface

+ Create New Edit Delete

Name	Virtual Switch	MAC	Model
port1	Bridge_Internal	00:00:00:00:00:00	virtio-net

OK Cancel

Installing Third Party VMs

Installing via ISO

This example uses the CentOS7 ISO image as an example, however this method is transferrable to other x86 based ISO install

A minimum of two disks are required for an ISO based install:

- The ISO image to perform the initial install boot from
- The disk to which the VM will be installed

Upload ISO Image

Select Virtual Machine > [Upload] and upload the chose ISO Image, in this example CentOS-7-x86_64-NetInstall-1511.iso.

FortiHypervisor 500D FHV5HD3916800061

Dashboard
System
Admin
Image
Virtual Machine

Upload Image

File Name: CentOS7_ISO
Storage: HDD1
Select File Name: Choose File CentOS-7-x86...l-1511.iso

OK Cancel

Create Installation disk

Create a disk to which the ISO image will be installed. Select the appropriate disk size according to the requirements of the Guest VM being installed.

FortiHypervisor 500D FHV5HD3916800061

Dashboard

System >

Admin >

Image

Virtual Machine

New Image

File Name: CentOS7_Disk

Storage: HDD1

Size (GB): 30

OK Cancel

Configure VM

Once the disks have been configured, proceed to the *Virtual Machine* > *[Create New]* to provision the VM.

- CPU:** Select the number of CPUs to suit your environment and VM license
- Memory:** Select the amount of memory to suit your environment and VM license
- Boot Order** Select the boot order of Hard-Disk or CDROM. In the ISO case, set this to CDROM
- License:** This is not relevant for an ISO install, leave empty.
- AutoStart:** Set start the VM once configuration has been completed.
- Disk:** Select Create New and bind the previously uploaded Boot disk and data disk(s) (VM dependent)
- Select the disk type according to the VM being configured.
 - For compatibility, set this to IDE.
 - For performance, set this to Virtio (if your VM supports this hardware type).
- Interface:** Select Create New and bind the appropriate Virtual Switch interfaces to the VM
- Select the interface type according to the VM being configured.
 - For compatibility, set this to E1000 (or RT8139).
 - For performance, set this to Virtio-net (if your VM supports this hardware type).

FortiHypervisor 500D FHV5HD3916800061

Dashboard
System
Admin
Image
Virtual Machine

Edit

Name: CentOS7
CPUs: 1
Memory(MB): 1024
Boot Order: CD-ROM
License: none

☒ Auto Start

Disk

+ Create New
Edit
Delete

Name	File	Type	Interface
disk1	/HDD1/CentOS7_Disk	disk	virtio
disk2	/HDD1/CentOS_7_ISO	cdrom	virtio

Interface

+ Create New
Edit
Delete

Name	Virtual Switch	MAC	Model
port1	Bridge_Internal	00:00:00:00:00:00	virtio-net

OK Cancel

On completion the ISO will begin to boot. Select the VM and click [_Console]

FortiHypervisor 500D FHV5HD3916800061												Interim	admin
Dashboard	<div> Import + Create New Edit Delete </div> <div> Console Start Pause Shutdown Poweroff </div>												
System	ID	Name	Auto Start	CPUs	Memory	CPU Usage	Memory Usage	Disk	Interfaces	Boot Order	License	Status	
Admin	1	FortiOS_5.6_Beta2_Boot	enable	1	1024	N/A	N/A	disk1	port1 port2	disk		Powered Off	
Image	2	FortiMail	enable	1	1024	N/A	N/A	disk1 disk2	port1	disk		Powered Off	
Virtual Machine	3	CentOS7	enable	1	1024	0%	0%	disk1 disk2	port1	cdrom		Running	

Follow the ISO install instructions or on-screen commands to complete the VM install process.

Once the installation is complete, power off the VM and change the boot order to prioritize boot from Hard Disk instead of CDROM. The CDROM drive can be removed if no longer required.

FortiHypervisor Administration Guide 1.0
Fortinet Technologies Inc.

26

Appendix A

Tested Fortinet VM Configurations

VM	Disk	Network	Notes
FortiManager KVM 5.4.1	Virtio	Virtio-net	
FortiAnalyzer KVM 5.4.1	Virtio	Virtio-net	
FortiGate KVM 5.4.1	Virtio	Virtio-net	
FortiWeb KVM 5.6.0	Virtio	Virtio-net	
FortiADC KVM 4.6.0	Virtio	Virtio-net	
FortiRecorder KVM 2.4.1	Virtio	Virtio-net	
FortiVoice KVM 5.2.2	Virtio	Virtio-net	
FortiMail KVM 5.3.6	Virtio	Virtio-net	
FortiCache KVM 4.1.4	IDE	E1000	Virtio to be supported in future FCH release.

Tested Third Party VM Configurations

Operating Systems

VM	Disk	Network	Notes
Windows Server 2012 R2	IDE	E1000	ISO Install
Windows 10 Pro	IDE	E1000	ISO Install
Windows 7 Pro	IDE	E1000	ISO Install
CentOS 7	Virtio	Virtio-net	ISO Install from Netinstall image (Install Type Network Server with GUI)
Ubuntu 16.04	Virtio	Virtio-net	ISO Install from Netinstall image (Install Type Network Server with GUI)
Tiny Core Linux 6.4	Virtio	Virtio-net	Prebuilt KVM
Alpine Linux 3.2.3	IDE	Virtio-net	Prebuilt KVM
CirrOS 0.3.4	IDE	E1000	Prebuilt KVM (OpenStack)
OpenBSD 6.0	IDE	E1000	ISO Install
VMWare ESXi 6.5	IDE	E1000	ISO Install

Application VMs and VNFs

VM	Disk	Network	Notes
VeloCloud SD-WAN	Virtio	Virtio-net	



FORTINET

High Performance Network Security



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.